Non-Normalized Walsh-Hadamard Transforms, Carry Accumulation, and Random Number Generation

Overview

The Fast Walsh-Hadamard Transform (FWHT) is normally viewed as a linear orthogonal transform after normalization. For transform size $N=2^k$

$H^N H^{NT} = NI$.

Most treatments focus on the normalized transform

$1/\text{sqrt}(N) H^N$.

However, for integer computation it may be more interesting to consider the *non-normalized* transform operating directly on machine integers.

Integer Butterfly Structure

The fundamental butterfly is

$u = a + b$, $v = a - b$.

This operation is inexpensive and consists only of additions and subtractions.

For a transform of size N, each output becomes a signed sum of N inputs. Consequently, the dynamic range grows by approximately log_2(N) bits.

For example, a 16-point transform can generate values requiring up to 4 additional bits compared to the original word size.

Hidden State in Carry Accumulation

A conventional linear analysis treats the transform as a matrix multiplication. On actual hardware this misses an important effect: carry generation.

Each addition creates carry information that may extend beyond the nominal word width. During a full FWHT, many such additions occur in a structured hierarchy.

The transform therefore temporarily generates information in higher-order bits that were not explicitly represented in the original state words.

This suggests viewing the FWHT as a mechanism for:

1. Global state diffusion.
2. Carry accumulation.
3. Temporary state expansion.

If overflow bits are retained, recycled, or fed back into the state, the transform is no longer adequately described by linear algebra alone.

Relation to Gaussian Behavior

Each output of an FWHT is a signed sum of many inputs.

For independent inputs,

$s = \text{sum of } \pm x_i$

the Central Limit Theorem suggests that the distribution of s approaches a Gaussian as the transform size increases.

Consequently:

- Carry counts may exhibit approximately Gaussian statistics.
- High-order overflow bits may contain aggregate information from many state variables.
- Carry channels may represent a compressed summary of global state interactions.

This is analogous to how multiplication derives much of its mixing power from carry propagation.

Potential RNG Architecture

A possible round structure is:

1. XOR or Weyl perturbation.
2. Non-normalized FWHT.

3. Capture overflow or carry bits.
4. Optional normalization by power-of-two shift.
5. Feedback of carry information into state.

Example:

```
state ^= constants
FWHT(state)
carry_state ^= high_bits(state)
normalize(state)
state ^= carry_state
```

The FWHT provides global diffusion while carry feedback introduces nonlinearity.

Research Directions

1. Carry Statistics

Measure:

- Overflow frequency.
- Carry-bit entropy.
- Distribution of carry channels.

Determine whether the distributions converge toward Gaussian forms as transform size increases.

2. State-Dependent Sign Matrices

Investigate transforms of the form

$$x_{n+1}=HD(x_n)x_n$$

where (D) is a diagonal matrix with entries ±1 selected from state bits.

This creates a large family of dynamically changing transforms rather than a single fixed operator.

3. Resonance and Eigenmode Suppression

Fixed Hadamard transforms possess strong algebraic structure and invariant modes.

Study whether:

- XOR constants,
- Weyl increments,
- carry feedback,

effectively destroy these resonances.

4. Overflow-State Generators

Treat overflow bits as an auxiliary state variable.

Questions include:

- Does auxiliary carry state increase effective state complexity?
- Does it improve resistance to linear analysis?
- Can it increase practical period?

5. Comparison with Multiplicative Mixers

Compare FWHT carry accumulation against multiplication by large odd constants.

Metrics:

- Avalanche behavior.
- Statistical quality.
- Computational cost.
- Diffusion rate.

Conclusion

The non-normalized FWHT may be viewed not merely as a linear transform but as a mechanism for generating and redistributing carry information. While the transform itself is algebraically simple, the interaction between carry accumulation, truncation, feedback, and dynamically changing sign patterns may create behavior substantially richer than conventional linear analyses suggest. This appears to be a largely unexplored area between classical Walsh transforms, ARX designs, and counter-based random number generators.